

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

1300 I STREET, N. W.
WASHINGTON, DC 20005-3315

202 • 408 • 4000
FACSIMILE 202 • 408 • 4400

WRITER'S DIRECT DIAL NUMBER:

RECEIVED

JUN 07 2000

Group 2700

TOKYO

011 • 813 • 3431 • 6943

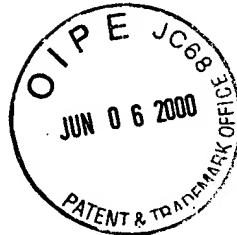
BRUSSELS

011 • 322 • 646 • 0353

ATLANTA
404 • 653 • 6400
PALO ALTO
650 • 849 • 6600

ATTORNEY DOCKET NO. 04329.2231

Assistant Commissioner
for Patents
Washington, D.C. 20231



U.S. Patent Application for: Personal Authentication System and Portable Unit
and Storage Medium Used Therefor

Inventors: Miki Yamada et al.

Serial No.: 09/506,377

Filed: February 18, 2000

Group Art Unit: 2766

CLAIM FOR PRIORITY

Sir:

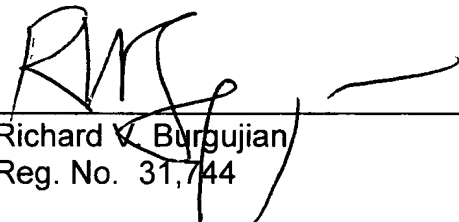
Under the provisions of Section 119 of 35 U.S.C., applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 11-041564 filed February 19, 1999, for the above identified United States Patent Application.

In support of applicants claim for priority, filed herewith is one certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW
GARRETT & DUNNER, L.L.P.

by:


Richard V. Burgujian
Reg. No. 31,744

Dated: JUNE 06, 2000

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 2月 19日

出 願 番 号
Application Number:

平成11年特許願第041564号

出 願 人
Applicant (s):

株式会社東芝

RECEIVED

JUN 07 2000

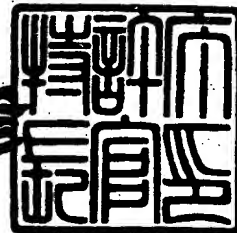
Group 2700

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 3月 3日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



【書類名】 特許願

【整理番号】 A009900781

【提出日】 平成11年 2月19日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 11/00
G06K 7/00

【発明の名称】 個人認証システム、それに使用される携帯装置及び記憶媒体

【請求項の数】 6

【発明者】

 【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

 【氏名】 山田 貢己

【発明者】

 【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

 【氏名】 森尻 智昭

【発明者】

 【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

 【氏名】 才所 敏明

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 個人認証システム、それに使用される携帯装置及び記憶媒体

【特許請求の範囲】

【請求項 1】 耐タンパー性を有し、登録情報の記憶された携帯装置と、耐タンパー性を有し、前記携帯装置との間で通信が可能なとき、前記携帯装置内の登録情報と新規に入力される入力情報とに基づいて、個人認証を実行可能な個人認証装置とを備えた個人認証システムであって、

前記携帯装置は、前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記個人認証装置に与える暗号化手段を有し、

前記個人認証装置は、

前記暗号化手段から与えられた暗号文を復号して登録情報を得る復号手段と、前記復号手段により得られた登録情報と前記入力情報とを照合する照合手段とを備えたことを特徴とする個人認証システム。

【請求項 2】 請求項 1 に記載の個人認証システムに使用される携帯装置であって、

前記個人認証が実行されるとき、乱数を生成する乱数生成手段と、

前記乱数生成手段により生成された乱数により前記登録情報を暗号化して得られた暗号文と前記乱数を前記個人認証装置の鍵で暗号化して得られた暗号文とを夫々前記個人認証装置に与える前記暗号化手段と

を備えたことを特徴とする携帯装置。

【請求項 3】 請求項 1 に記載の個人認証システムに使用されるコンピュータ読取り可能な記憶媒体であって、

前記携帯装置内のコンピュータに、

前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記個人認証装置に与える暗号化手順を実行させ、

前記個人認証装置内のコンピュータに、

前記暗号化手段から与えられた暗号文を復号して登録情報を得る復号手順を実行させ、

前記復号手順により得られた登録情報と前記入力情報とを照合する照合手順を実行させる

ためのプログラムを記憶したコンピュータ読取り可能な記憶媒体。

【請求項4】 耐タンパー性を有し、登録情報の記憶された携帯装置と、耐タンパー性を有し、前記携帯装置との間で通信が可能なとき、前記携帯装置内の登録情報と新規に入力される入力情報とに基づいて、個人認証を実行可能な一つ或いは複数の個人認証装置と、耐タンパー性を有し、前記携帯装置と前記各個人認証装置との間にて暗号化を含む転送処理を行なう固設部とを備えた個人認証システムであって、

前記携帯装置は、前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記固設部に与える第1暗号化手段を備え、

前記固設部は、

前記第1暗号化手段から与えられた暗号文を復号して登録情報を得る第1復号手段と、

前記第1復号手段により得られた登録情報を予め設定された暗号鍵により暗号化し、得られた暗号文を送出する第2暗号化手段とを備え、

前記各個人認証装置は、移動可能に配置され、

前記第2暗号化手段から送出された暗号文を予め設定された暗号鍵により復号して登録情報を得る第2復号手段と、

前記第2復号手段により得られた登録情報と前記入力情報とを照合する照合手段と

を備えたことを特徴とする個人認証システム。

【請求項5】 請求項4に記載の個人認証システムに使用される携帯装置であって、

前記個人認証が実行されるとき、乱数を生成する乱数生成手段と、

前記乱数生成手段により生成された乱数により前記登録情報を暗号化して得られた暗号文と前記乱数を前記固設部の鍵で暗号化して得られた暗号文とを夫々前記固設部に与える前記第1暗号化手段と

を備えたことを特徴とする携帯装置。

【請求項 6】 請求項 4 に記載の個人認証システムに使用されるコンピュータ読取り可能な記憶媒体であって、

前記携帯装置内のコンピュータに、

前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記固設部に与える第 1 暗号化手順を実行させ、

前記固設部のコンピュータに、

前記第 1 暗号化手順により与えられた暗号文を復号して登録情報を得る第 1 復号手順を実行させ、

前記第 1 復号手順により得られた登録情報を予め設定された暗号鍵により暗号化し、得られた暗号文を送出する第 2 暗号化手順を実行させ、

前記各個人認証装置のコンピュータに、

前記第 2 暗号化手順により送出された暗号文を予め設定された暗号鍵により復号して登録情報を得る第 2 復号手順を実行させ、

前記第 2 復号手順により得られた登録情報と前記入力情報とを照合する照合手順を実行させる

ためのプログラムを記憶したコンピュータ読取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、例えば IC カードの如き携帯可能な装置を用いる個人認証システム、それに使用される携帯装置及び記憶媒体に係り、特に、盗聴による不正を阻止し得る個人認証システム、それに使用される携帯装置及び記憶媒体に関する。

【0002】

【従来の技術】

一般に、個人の権限の正当性を認証する分野では、商取引でのクレジットカードや立入制限場所での入退室管理カードの如き、携帯可能な ID カードを持参した個人に関してその権限の正当性を認証するための個人認証システムが広く用いられている。

【0003】

この種のＩＤカードとしては、通常、磁気カードが使用される。また最近では、半導体チップの内蔵により、高セキュリティ性と高機能とを持つＩＣカードが使用され始めている。このＩＣカードは、磁気カードに比べて内部情報の読出／書込が困難であるため、偽造や情報漏洩などの不正を防止可能である旨が期待される。

【０００４】

但し、このようなＩＣカードは、単に内部情報を保持する構成のとき、紛失や盗難により他人に不正使用されたり、紛失と偽って不正使用される形態の不正を防止することが困難である。

よって、係る不正を防止する観点から、ＩＣカードでは、内部に個人認証情報が登録された構成とされる。これにより、個人認証装置の照合部では、ＩＣカードから送信された個人認証情報と、別途、操作入力された入力情報とが照合され、ＩＣカードを持参した者の権限の正当性が判定される。なお、個人認証情報はパスワードのようなものでもよい。

【０００５】

【発明が解決しようとする課題】

しかしながら、以上のような個人認証システムでは、ＩＣカードと照合部との間の通信内容が盗聴されることにより、不正に個人認証情報が読出されて不正使用されるという可能性がある。

【０００６】

本発明は上記実情を考慮してなされたもので、携帯装置と個人認証装置との間が盗聴されても、盗聴内容から情報を読出せず、その不正使用を阻止し得る個人認証システム、それに使用される携帯装置及び記憶媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】

請求項１に対応する発明は、耐タンパー性を有し、登録情報の記憶された携帯装置と、耐タンパー性を有し、前記携帯装置との間で通信が可能なとき、前記携帯装置内の登録情報と新規に入力される入力情報とに基づいて、個人認証を実行

可能な個人認証装置とを備えた個人認証システムであって、前記携帯装置としては、前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記個人認証装置に与える暗号化手段を有し、前記個人認証装置としては、前記暗号化手段から与えられた暗号文を復号して登録情報を得る復号手段と、前記復号手段により得られた登録情報と前記入力情報とを照合する照合手段とを備えた個人認証システムである。

【 0 0 0 8 】

また、請求項 2 に対応する発明は、請求項 1 に対応する個人認証システムに使用される携帯装置であって、前記個人認証が実行されるとき、乱数を生成する乱数生成手段と、前記乱数生成手段により生成された乱数により前記登録情報を暗号化して得られた暗号文と前記乱数を前記個人認証装置の鍵で暗号化して得られた暗号文とを夫々前記個人認証装置に与える前記暗号化手段とを備えた携帯装置である。

【 0 0 0 9 】

さらに、請求項 3 に対応する発明は、請求項 1 に対応する個人認証システムに使用されるコンピュータ読取り可能な記憶媒体であって、前記携帯装置内のコンピュータに、前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記個人認証装置に与える暗号化手順を実行させ、前記個人認証装置内のコンピュータに、前記暗号化手段から与えられた暗号文を復号して登録情報を得る復号手順を実行させ、前記復号手順により得られた登録情報と前記入力情報とを照合する照合手順を実行させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体である。

【 0 0 1 0 】

また、請求項 4 に対応する発明は、耐タンパー性を有し、登録情報の記憶された携帯装置と、耐タンパー性を有し、前記携帯装置との間で通信が可能なとき、前記携帯装置内の登録情報と新規に入力される入力情報とに基づいて、個人認証を実行可能な一つ或いは複数の個人認証装置と、耐タンパー性を有し、前記携帯装置と前記各個人認証装置との間にて暗号化を含む転送処理を行なう固設部とを備えた個人認証システムであって、前記携帯装置としては、前記個人認証が実行

されるとき、前記登録情報を暗号化し、得られた暗号文を前記固設部に与える第 1 暗号化手段を備え、前記固設部としては、前記第 1 暗号化手段から与えられた暗号文を復号して登録情報を得る第 1 復号手段と、前記第 1 復号手段により得られた登録情報を予め設定された暗号鍵により暗号化し、得られた暗号文を送出する第 2 暗号化手段とを備え、前記各個人認証部としては、移動可能に配置され、前記第 2 暗号化手段から送出された暗号文を予め設定された暗号鍵により復号して登録情報を得る第 2 復号手段と、前記第 2 復号手段により得られた登録情報と前記入力情報とを照合する照合手段とを備えた個人認証システムである。

【 0 0 1 1 】

さらに、請求項 5 に対応する発明は、請求項 4 に対応する個人認証システムに使用される携帯装置であって、前記個人認証が実行されるとき、乱数を生成する乱数生成手段と、前記乱数生成手段により生成された乱数により前記登録情報を暗号化して得られた暗号文と前記乱数を前記固設部の鍵で暗号化して得られた暗号文とを夫々前記固設部に与える前記第 1 暗号化手段とを備えた携帯装置である。

【 0 0 1 2 】

また、請求項 6 に対応する発明は、請求項 4 に対応する個人認証システムに使用されるコンピュータ読取り可能な記憶媒体であって、前記携帯装置内のコンピュータに、前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記固設部に与える第 1 暗号化手順を実行させ、前記固設部のコンピュータに、前記第 1 暗号化手順により与えられた暗号文を復号して登録情報を得る第 1 復号手順を実行させ、前記第 1 復号手順により得られた登録情報を予め設定された暗号鍵により暗号化し、得られた暗号文を送出する第 2 暗号化手順を実行させ、前記各個人認証装置のコンピュータに、前記第 2 暗号化手順により送出された暗号文を予め設定された暗号鍵により復号して登録情報を得る第 2 復号手順を実行させ、前記第 2 復号手順により得られた登録情報と前記入力情報とを照合する照合手順を実行させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体である。

【 0 0 1 3 】

(作用)

従って、請求項 1, 3 に対応する発明は以上のような手段を講じたことにより、携帯装置の暗号化手段が、個人認証が実行されるとき、登録情報を暗号化し、得られた暗号文を個人認証装置に与え、個人認証装置の復号手段が、暗号化手段から与えられた暗号文を復号して登録情報を得ると、照合手段が、復号手段により得られた登録情報と入力情報とを照合するので、携帯装置と個人認証装置との間が盗聴されても、盗聴内容から情報を読出せず、その不正使用を阻止することができる。

【0014】

また、請求項 4, 6 に対応する発明は、携帯装置の第 1 暗号化手段が、個人認証が実行されるとき、登録情報を暗号化し、得られた暗号文を固設部に与え、固設部としては、第 1 復号手段が、第 1 暗号化手段から与えられた暗号文を復号して登録情報を得ると、第 2 暗号化手段が、第 1 復号手段により得られた登録情報を予め設定された暗号鍵により暗号化し、得られた暗号文を送出し、各個人認証装置の第 2 復号手段が、第 2 暗号化手段から送出された暗号文を予め設定された暗号鍵により復号して登録情報を得ると、照合手段が、第 2 復号手段により得られた登録情報と入力情報とを照合するので、請求項 1, 3 に対応する作用に加え、各個人認証装置の接続の変更や固設部の暗号鍵の交換の場合でも、個人認証装置の同一性を保証でき、安全性を保持することができる。

【0015】

また、請求項 2, 5 に対応する発明は、携帯装置において、乱数生成手段が、個人認証が実行されるとき、乱数を生成し、暗号化手段が、乱数生成手段により生成された乱数により登録情報を暗号化して得られた暗号文と乱数を個人認証装置又は固設部の鍵で暗号化して得られた暗号文とを夫々個人認証装置又は固設部に与えるので、請求項 1, 4 に対応する作用に加え、登録情報の暗号化鍵の変更が容易で、盗聴などによる登録情報の漏洩を阻止でき、内部情報の漏洩による影響を最小限に抑制でき、暗号解読攻撃に対して防御性を向上させることができる。

【0016】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照しながら説明する。具体的には、以下の各実施形態では、最近注目されてきたバイオメトリクス技術を考慮し、従来のパスワードに代えて、個人の生体データを用いた場合について述べる。なお、バイオメトリクスは、生体データを用いて人間を認識する技術であり、例えば指紋認識、音声認識、手書き署名認識、網膜走査認識、及び手の幾何学的認識（掌型や指の長さ等）などがその技術範囲に含まれる。但し、パスワードを用い、パスワードと入力データとを照合する構成としても各実施形態は有効である。

【0017】

（第1の実施形態）

図1は本発明の第1の実施形態に係る個人認証システムの構成を示す模式図である。この個人認証システムは、耐タンパー性を有するICカード10と、耐タンパー性を有するセンサユニット20との2種類を主要な構成要素として有している。

【0018】

なお、耐タンパー性は、内部情報の盗み見や改ざんから防御する性質であり、例えば不正なアクセス時に内部情報が消去される等の周知の機能を付加することにより、実現可能となっている。

【0019】

係る個人認証システムは、具体的には、演算処理や表示処理等の通常の計算機機能の他、挿入されたICカード（携帯装置）10に対して情報を読出／書込可能なリーダライタ機能、センサユニット20並びに業務ソフトウェア30を有するクライアント装置40を備えている。なお、リーダライタ機能は、別体の装置として設けてもよい。このクライアント装置40及びICカード10は、例えば磁気ディスク等の記憶媒体に記憶されたプログラムを読み込み、このプログラムによって動作が制御されるコンピュータによって実現される。但し、ICカード10は、生体データの登録の際にプログラムが読込まれ、以後、そのプログラムに基づいて動作する。

【0020】

ここで、ICカード10は、耐タンパー性を有し、生成データ記憶部11、認証部12、暗号鍵記憶部13及び暗号化部14を備えている。生体データ記憶部11は、予め個人の生体データが読出可能に記憶されたものである。生体データとしては、例えば指紋データ、音声（声紋）データ、手書き署名データ、網膜パターンデータ、又は手の幾何学データなどが適宜使用可能となっている。なお、ICカードは、プログラムの読込に限らず、予め設計されたファームウェアを用いて実現してもよい。

【0021】

認証部12は、センサユニット20との間で相互認証を行うためのものであり、自己（ICカード）の正当性を証明するための証明書15と、センサユニット20から送られる証明書を検証するための認証局の公開鍵Paと、復号された内容を照合するための認証局名と、自己の秘密鍵Siとを有している。

【0022】

証明書15は、少なくともICカードの公開鍵Piの値、証明書15を発行した認証局名、及びPiの値と前記認証局名の組を認証局の秘密鍵Saでデジタル署名した署名の3つを有する。

【0023】

認証部12は、具体的には、ICカード10がクライアント装置40に挿入されたとき、センサユニット20の証明書を検証する機能と、センサユニット20に関してセンサユニット20の秘密鍵Ssを有する旨を認証する機能と、センサユニット20からICカード10の秘密鍵Siを有する旨を認証されるための機能とをもっている。

【0024】

認証部12において、センサユニット20の証明書を検証する機能は、証明書15をセンサユニット20に送出する機能と、センサユニット20から受けた証明書を認証局の公開鍵Paを用いて検証し、復号結果を認証局名を用いて真偽判定する機能とからなる。

【0025】

認証部12において、センサユニット20にてその秘密鍵Ssを有する旨を認

証する機能は、証明書の検証における判定結果が“真”のとき、新規に暗号鍵R（疑似乱数）を生成する機能と、その暗号鍵Rをセンサユニット20の証明書から得たセンサユニット20の公開鍵P_sで暗号化し、得られた暗号文P_s[R]をセンサユニット20に送出する機能と、センサユニット20から受けた暗号文P_i[R]を自己の秘密鍵S_iで復号して得られた暗号鍵Rを自己の送出した暗号鍵Rに一致するか否かを判定する機能とからなり、判定結果が“真”のとき、その暗号鍵Rを暗号鍵記憶部13に書込むようにしている。

【0026】

なお、暗号鍵Rは、疑似乱数に限らないが、過去にその都度生成した暗号鍵Rによる暗号文R[D]の集合から予測不可能とする観点により疑似乱数が好ましい。

【0027】

認証部12において、センサユニット20から自己が秘密鍵S_iをもつ旨を認証される機能は、センサユニット20から受けたメッセージM1を含む返信M1+M2を作成し、M1+M2を自己の秘密鍵S_iにて署名した署名S_i[M1+M2]、自己の証明書15と共に乱数Rで暗号化してR[M1+M2+S_i[M1+M2]+証明書15]を作成し、センサユニット20の証明書から得たセンサユニット20の公開鍵P_sでRを暗号化したP_s[R]と共にセンサユニットに送出する機能とからなる。なお、R[M1+M2+S_i[M1+M2]+証明書15]+P_s[R]を以後、デジタル封書DE[M1+M2, S_i, P_s; R]と呼ぶ。

【0028】

暗号鍵記憶部13は、暗号鍵Rが暗号化部14から読出可能に記憶されるものである。

【0029】

暗号化部14は、生体データ記憶部11内の生体データDを暗号鍵記憶部13内の暗号鍵Rにより暗号化してなる暗号文R[D]をセンサユニット20内の復号部23に送出する機能をもっている。

【0030】

センサユニット 20 は、耐タンパー性を有し、認証部 21、復号鍵記憶部 22、復号部 23、センサ 24、照合部 25 及び演算部 26 を備えている。

【0031】

ここで、認証部 21 は、IC カード 10 との間で相互認証を行うためのものであり、自己（センサユニット）の正当性を証明するための証明書 27 と、IC カード 10 から送られる証明書 15 を検証するための認証局の公開鍵 P_a と、復号された内容を照合するための認証局名と、自己の秘密鍵 S_s とを有している。ここで、証明書 27 は、少なくともセンサユニット 20 の公開鍵 P_s の値、証明書 27 を発行した認証局名、及び P_s の値と前記認証局名の組を認証局の秘密鍵 S_a でデジタル署名した署名の 3 つを有する。

【0032】

認証部 21 は、具体的には、IC カード 10 がクライアント装置 40 に挿入されたとき、IC カード 10 の証明書 15 を検証する機能と、IC カード 10 に関して IC カード 10 の秘密鍵 S_i を有する旨を認証する機能と、IC カード 10 からセンサユニット 20 の秘密鍵 S_s を有する旨を認証されるための機能とをもっている。

【0033】

認証部 21 において、IC カード 10 の証明書 15 を検証する機能は、証明書 27 を IC カード 10 に送出する機能と、IC カード 10 から受けた証明書 15 を認証局の公開鍵 P_a を用いて復号し、復号結果を認証局名を用いて真偽判定する機能とからなる。

【0034】

認証部 12 において、IC カード 10 にてその秘密鍵 S_i を有する旨を認証する機能は、毎回異なるような（例えば乱数、時刻などを含む）メッセージ M_1 を作成し、 M_1 を IC カード 10 に送出する機能と、IC カード 10 から受けたデジタル封書 $DE [M_1 + M_2, S_i, P_s; R]$ を自己の秘密鍵 S_s で復号して得られたメッセージ M_1 が自己の送出した M_1 に一致するか否かを判定する機能と、デジタル封書 $[M_1 + M_2, S_i, P_s; R]$ に含まれる証明書 15 の判定結果が“真”のとき、デジタル封書 $[M_1 + M_2, S_i, P_s; R]$ に含まれる

署名 S_i [$M1+M2$] が IC カード 10 が署名したものであることを検証する機能とからなり、 $M1$ の判定結果が “真” で、且つ、IC カード 10 が署名したことを検証できたとき、IC カード 10 の認証処理を終了し、“偽”、又は、検証できなかったとき、エラー表示信号を発生して処理を終了するようにしている。

【0035】

認証部 21 において、IC カード 10 からセンサユニット 20 の秘密鍵 S_s を有する旨を認証される機能は、IC カード 10 から受けた暗号文 P_s [R] を自己の秘密鍵 S_s で復号し、得られた暗号鍵 R を IC カード 10 の証明書から得た IC カード 10 の公開鍵 P_i で暗号化し、得られた暗号文 P_i [R] を IC カード 10 に送出する機能と、その暗号鍵 R を復号鍵記憶部 22 に書込む機能とをもっている。

【0036】

復号鍵記憶部 22 は、認証部 21 から書込まれた暗号鍵 R を復号部 23 から読出可能に記憶するものである。

【0037】

復号部 23 は、IC カード 10 の暗号化部 14 から暗号文 R [D] を受けると、復号鍵記憶部 22 内の暗号鍵 R により暗号文 R [D] を復号し、得られた生体データ D を照合部 25 に与える機能をもっている。

【0038】

センサ 24 は、ユーザ（IC カード携帯者）の生体測定を行ない、測定結果を電子化して生体測定データ D_m を作成してこの生体測定データ D_m を照合部 25 に与える機能をもっている。

【0039】

照合部 25 は、センサ 24 から受けた生体測定データ D_m と復号部 23 から受けた生体データ D とを照合し、両者が一致したとき、許可データを演算部 26 に与える機能と、両者が不一致のとき、エラー表示信号を発生する機能とをもっている。なお、センサ 24 及び照合部 25 は、指紋照合装置や掌型照合装置などが適宜使用可能となっている。

【0 0 4 0】

演算部 2 6 は、照合部 2 5 から受けた許可データを演算し、得られた結果データを業務ソフトウェア 3 0 に与える機能をもっている。

業務ソフトウェア 3 0 は、演算部 2 6 から結果データを受けると実行可能となる任意の内容のアプリケーションであり、例えば会計処理用プログラムやプラント制御用プログラムといった任意の計算機ソフトウェアが使用可能である。

【0 0 4 1】

次に、以上のように構成された個人認証システムの動作を図 2 のフローチャートを用いて説明する。なお、ここでは、会社のクライアント／サーバシステム上の業務ソフトウェア 3 0 を起動して端末業務を開始する際に、IC カード 1 0 によりユーザを確認する場合を例に挙げて述べる。

クライアント装置 4 0 は、ユーザの操作により電源が投入され、コマンドやユーザ ID の入力要求等の指示を画面表示し、IC カード 1 0 の挿入を待つ。

続いて、クライアント装置 4 0 では、ユーザにより IC カード 1 0 が挿入されると (S T 1)、IC カード 1 0 とセンサユニット 2 0 との夫々の認証部 1 2, 2 1 が証明書の検証と、相互に秘密鍵を有する旨を認証する相互認証とを実行する (S T 2)。

【0 0 4 2】

ステップ S T 2 の相互認証を、具体的に、認証手順を示した図 3 を用いて説明する。

【0 0 4 3】

センサユニット 2 0 の認証部 2 1 は、IC カード 1 0 がクライアント装置 4 0 に挿入されたとき、証明書 2 7 と、毎回異なるような (例えば乱数、時刻などを含む) メッセージ M 1 とを IC カード 1 0 に送出する (S T 2 1)。M 1 は IC カード 1 0 の認証に用いられる。

【0 0 4 4】

次に、IC カード 1 0 の認証部 1 2 は、センサユニット 2 0 から受けた証明書 2 7 に含まれる認証局の署名を認証局の公開鍵 P a を用いて復号し、この復号結果を認証局名を用いて真偽判定し、判定結果が“真”のとき、証明書 2 7 の検証

を完了する (ST221)。

【0045】

次に、ICカード10の認証部12は、メッセージM1に対する返信M1+M2を作成し (ST222)、新規に暗号鍵Rを作成し (ST223)、証明書15を含むデジタル封書DE [M1+M2, Si, Ps; R] を作成し、センサユニットに送出する (ST224)。

【0046】

次に、センサユニット20の認証部21は、ICカード10から受けたデジタル封書DE [M1+M2, Si, Ps; R] を自己の秘密鍵Ssを用いて復号し、M1+M2と署名Si [M1+M2] とICカード10の証明書15と暗号鍵Rとを取得し (ST231)、証明書15に含まれる認証局の署名を認証局の公開鍵Paを用いて復号し、この復号結果を認証局名を用いて真偽判定し、判定結果が“真”のとき、証明書15の検証を完了する (ST232)。

【0047】

なお、いずれの認証部12, 21においても真偽判定の結果が“偽”を示すとき、エラー表示信号を発生して処理を終了する。

【0048】

次に、センサユニット20の認証部21は、ICカード10の署名Si [M1+M2] を証明書15から得られるICカード10の公開鍵Piで復号し、復号結果をM1+M2、あるいはM1+M2のメッセージダイジェストを用いて真偽判定し、また、センサユニットから受けたM1が自己の作成したM1と一致するか否かを真偽判定し、これら2つの判定結果が共に“真”のとき、ICカード10に関して、ICカード10の秘密鍵Siを有し、且つ、現在クライアント装置40に接続されている旨の認証を完了し、暗号鍵Rを復号鍵記憶部22に書込む。また、2つの判定結果のいずれかが“偽”のとき、エラー表示信号を発生して処理を終了する (ST233)。

【0049】

次に、センサユニット20の認証部21は、暗号鍵RをICカード10の公開鍵Piで暗号化し、得られた暗号文Pi [R] をICカード10に送出する (

ST234)。

【0050】

次に、ICカード10の認証部12は、センサユニット20から受けた暗号文 $P_i[R]$ を自己の秘密鍵 S_i で復号して得られた暗号鍵 R を自己の送出した暗号鍵 R に一致するか否かを判定し、判定結果“真”のとき、センサユニット20に関して、センサユニット20の秘密鍵 S_s を有し、且つ、現在クライアント装置40に接続されている旨の認証を完了し、暗号鍵 R を暗号鍵記憶部13に書込む。また、判定結果が“偽”のとき、エラー表示信号を発生して処理を終了する(ST24)と共に、ステップST2の相互認証の手順を終了する(ST2)。

【0051】

以上の相互認証の手順(ST2)は、互いの証明書を検証し合い、互いの認証を行い、暗号鍵 R を通信路に対して秘匿しつつ互いに共有することを行なう他の手順にて行ってもよい。

【0052】

次に、両認証部12, 21において、いずれも真偽判定の結果が“真”であり、相互認証が完了した場合について述べる。なお、この相互認証が完了した時点において、両認証部12, 21では、結果的に、新規に生成した乱数 R を共有しており、乱数 R を暗号用の鍵として使用可能としている。但し、相互認証の後、別に暗号鍵を生成してICカード10からセンサユニット20に送出してもよい。

【0053】

次に、ICカード10において、暗号化部14は、生体データ記憶部11内の生体データ D を暗号鍵記憶部13内の暗号鍵 R により暗号化し、得られた暗号文 $R[D]$ をセンサユニット20内の復号部23に与える(ST3)。

【0054】

センサユニット20においては、復号部23がこの暗号文 $R[D]$ を受けると、復号鍵記憶部22内の暗号鍵 R により暗号文 $R[D]$ を復号し(ST4)、得られた生体データ D を照合部25に与える。

【0055】

センサ 2 4 は、ユーザの指紋等の生体測定を行なう。生体測定は、例えば指紋を測定する場合、測定面上にユーザの指が乗せられて実行される。またセンサ 2 4 では、生体の測定信号が入力されると（S T 5）、その生体測定の結果を電子化して生体測定データ D m を作成し、この生体測定データ D m を照合部 2 5 に与える。

【 0 0 5 6 】

照合部 2 5 は、この生体測定データ D m と復号部 2 3 から受けた生体データ D とを照合して本人か否かを判定し（S T 6）、両データ D, D m が不一致のとき、“否”と判定してエラー表示信号を発生するが、両データ D, D m の一致により“本人”と判定されたとき、許可データを演算部 2 6 に与える。

【 0 0 5 7 】

演算部 2 6 は、この許可データを演算し（S T 7）、得られた結果データを業務ソフトウェア 3 0 に与える。業務ソフトウェア 3 0 は、演算部 2 6 から結果データを受けることにより、実行が開始される。

【 0 0 5 8 】

上述したように本実施形態によれば、I C カード 1 0 の暗号化部 1 4 が、個人認証が実行されるとき、生体データ D を暗号化し、得られた暗号文 R [D] をセンサユニット 2 0 に与え、センサユニット 2 0 の復号部 2 3 が、暗号文 R [D] を復号して生体データ D を得ると、照合部 2 5 が、この得られた生体データ D と入力された生体測定データ D m とを照合するので、I C カード 1 0 とセンサユニット 2 0 との間が盗聴されても、暗号文のために盗聴内容から情報を読出せず、その不正使用を阻止することができる。

【 0 0 5 9 】

また、I C カード 1 0 において、認証部 1 2 が暗号鍵 R（疑似乱数）を生成し、暗号化部 1 4 が、その暗号鍵 R をセンサユニット 2 0 の公開鍵 P s の鍵で暗号化して得られた暗号文 P s [R] と、その暗号鍵 R により生体データ D を暗号化して得られた暗号文 R [D] とを夫々センサユニット 2 0 に与えるので、生体データ D の暗号化鍵 R を容易に変更できることから、頻繁に暗号鍵 R を変更することにより、盗聴などによる生体データ D の漏洩やソフトウェア置換えによる不正

コマンド実行を阻止でき、暗号解読攻撃に対して防御性を向上させることができる。

【0060】

また、ICカード10とセンサユニット20とは相互認証を行うので、個人認証の確実性を向上させることができる。

【0061】

例えば、ステップST2の手順を採らずに、通常のデジタル封書処理（乱数で本文と署名と証明書を暗号化し、さらにその乱数を相手の公開鍵で暗号化する）により、ICカード10から生体データDをセンサユニット20に送出するだけでも、毎回異なる鍵を利用して暗号文を送ることができることから、今回の発明と似た効果を得られる。

【0062】

しかしながら、通常のデジタル封書処理では、その生体データDが現在得られたものか否かの保証がない。すなわち、クライアント装置にて不正に置換されたソフトウェアがセンサユニット20を騙そうとして、1週間前に得られたICカード10からの信号を保持しておき、その信号を今、センサユニット20に送り込んだ場合でも、センサユニット20がICカード10を現在挿入されていると判断してしまう問題がある。

【0063】

これに対し、本実施形態では、乱数のやり取りを含む前述した相互認証を行うことにより、その瞬間にICカード10が挿入されていることと、その瞬間にセンサユニット20が接続されていることとを確認できるので、より確実な本人確認を実行することができる。

【0064】

また、毎回、ICカード10が暗号鍵Rを生成し、センサユニット20に共有化させるので、特定のICカード10又はセンサユニット20の内部情報が漏洩したとしても、他のICカード10又はセンサユニット20の内部情報の連鎖的な漏洩を阻止することができる。

【0065】

さらに、センサユニット 2 0 の鍵ペア（公開鍵 P s - 秘密鍵 S s）及び I C カード 1 0 の暗号鍵 R を個別に更新できるので、便利で且つ暗号解読攻撃に対して強力な防御性を実現することができる。

【 0 0 6 6 】

また、バイオメトリクス技術を採用した場合、以上の効果に加え、パスワードを忘れたり、パスワードの書かれたメモを他人に読まれたり、といった可能性がないので、より一層、利便性を向上させることができる。

【 0 0 6 7 】

（第 2 の実施形態）

図 4 は本発明の第 2 の実施形態に係る個人検証システムの構成を示す模式図であり、図 1 と同一部分には同一符号を付してその詳しい説明を省略し、ここでは異なる部分について主に述べる。

【 0 0 6 8 】

本実施形態は、第 1 の実施形態の変形構成であり、複数のセンサユニット 2 0 B を接続可能として大規模化に対応した構成を示しており、クライアント装置 4 0 が、センサユニット 2 0 に代えて、耐タンパー性を有するクライアント認証部 2 0 A と、耐タンパー性を有するセンサユニット 2 0 B とを備えている。

【 0 0 6 9 】

すなわち、この個人認証システムにおいて、耐タンパー性を有する構成要素は、I C カード 1 0、クライアント認証部 2 0 A 及びセンサユニット 2 0 B の 3 種類である。

【 0 0 7 0 】

ここで、クライアント認証部 2 0 A は、I C カード 1 0 と相互認証を行い、I C カード 1 0 から受けた暗号文を復号してこの復号結果を共通鍵で暗号化し、この暗号文をセンサユニット 2 0 B に与える機能をもっている。

【 0 0 7 1 】

具体的には、クライアント認証部 2 0 A は、耐タンパー性を有し、認証部 2 1、復号鍵記憶部 2 2、復号部 2 3 a、共通鍵記憶部 2 8 a、暗号化部 2 9 を備えている。なお、認証部 2 1 及び復号鍵記憶部 2 2 は、前述同様の機能をもつもの

である。

【0072】

復号部 2 3 a は、前述同様の復号機能を有し、得られた生体データ D を暗号化部 2 9 に与える機能をもっている。

【0073】

共通鍵記憶部 2 8 a は、図示しない管理ソフトウェアから与えられる共通鍵 C k が暗号化部 2 9 から読出可能に記憶されるものである。なお、管理ソフトウェアは、権限ある管理者のみが取扱うソフトウェアであり、クライアント装置 4 0 A 内にあっても、他のサーバ装置（図示せず）内にあってもよい。

【0074】

暗号化部 2 9 は、復号部 2 3 a から受けた生体データ D を共通鍵記憶部 2 8 a 内の共通鍵 C k により暗号化し、得られた暗号文 C k [D] をセンサユニット 2 0 B 内の復号部 2 3 b に与える機能をもっている。

【0075】

センサユニット 2 0 B は、耐タンパー性を有し、共通鍵記憶部 2 8 b、復号部 2 3 b、センサ 2 4、照合部 2 5 及び演算部 2 6 を備えている。

共通鍵記憶部は、図示しない管理ソフトウェアから与えられる共通鍵 C k が復号部から読出可能に記憶されるものである。

【0076】

復号部 2 3 b は、クライアント認証部 2 0 A の暗号化部 2 9 から暗号文 C k [D] を受けると、共通鍵記憶部 2 8 b 内の共通鍵 C k により暗号文 C k [D] を復号し、得られた生体データ D を照合部 2 5 に与える機能をもっている。

センサ 2 4、照合部 2 5 及び演算部 2 6 は、前述同様の機能をもつものである。

【0077】

次に、以上のように構成された個人認証システムの動作を図 5 のフローチャートを用いて説明する。

ステップ S T 1 ～ S T 4 の復号処理までは、前述同様に行われる。

すなわち、クライアント装置 4 0 A の復号部 2 3 a は、前述同様の復号機能を

有し、ＩＣカード１０の暗号化部１４から暗号文Ｒ〔Ｄ〕を受けると、復号鍵記憶部２２内の暗号鍵Ｒにより暗号文Ｒ〔Ｄ〕を復号する（ＳＴ４）。

【００７８】

但し、復号部２３ａは、得られた生体データＤを暗号化部２９に与える。

暗号化部２９は、復号部２３ａから受けた生体データＤを共通鍵記憶部２８ａ内の共通鍵Ｃｋにより暗号化して得られた暗号文Ｃｋ〔Ｄ〕をセンサユニット２０Ｂ内の復号部２３ｂに与える（ＳＴ４ａ）。

【００７９】

センサユニット２０Ｂでは、復号部２３ｂが、クライアント認証部２０Ａの暗号化部２９から暗号文Ｃｋ〔Ｄ〕を受けると、共通鍵記憶部２８ｂ内の共通鍵Ｃｋにより暗号文Ｃｋ〔Ｄ〕を復号し（ＳＴ４ｂ）、得られた生体データＤを照合部２５に与える。

【００８０】

以下、前述同様にステップＳＴ５～ＳＴ７が実行され、正当なユーザである場合、業務ソフトウェア３０の実行が開始される。

上述したように本実施形態によれば、複数のセンサユニット２０Ｂを有する場合であっても、各センサユニット２０Ｂとクライアント認証部２０Ａとを共通鍵方式により結合することにより、第１の実施形態の効果をを得ることができ、さらに、各センサユニット２０Ｂの接続の変更やクライアント認証部２０Ａの暗号鍵の交換の場合でも、クライアント装置４０Ａの同一性を保証できるので、安全性を保持することができる。

【００８１】

また同様に、耐タンパー性をもつクライアント認証部２０Ａが認証処理を行なうので、複数のセンサユニット２０Ｂが接続されていたり、各センサユニット２０Ｂが着脱自在であっても、認証処理の安全性を確保することができる。

【００８２】

また、１つのクライアント認証部２０Ａが認証処理を行うことにより、複数のセンサユニット２０Ｂ及び複数のＩＣカード１０を有する大規模な構成の場合であっても、暗号鍵の更新の際に、クライアント認証部２０Ａの鍵ペア（公開鍵Ｐ

s-秘密鍵 S s)のみを更新すれば、その更新した公開鍵 P sを、相互認証の際に ICカード 10 に伝送できるので、暗号鍵の更新が容易であり、便利である。

【0083】

(他の実施形態)

なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピーディスク、ハードディスクなど）、光ディスク（CD-ROM、DVD など）、光磁気ディスク（MO）、半導体メモリなどの記憶媒体に書込んで各種装置に適用したり、通信媒体により伝送して各種装置に適用することも可能である。

【0084】

また、上記各実施形態では、照合部 25 が演算部 26 を介して結果情報を出力する場合について説明したが、これに限らず、演算部 26 が、ICカード 10 の公開鍵 P i を用いて演算結果を暗号化して ICカード 10 に送出し、ICカード 10 がサーバ装置（図示せず）を介して業務ソフトウェア 30 を起動する構成により、業務ソフトウェア 30 の実行を開始する際に業務ソフトウェア 30 には演算結果を秘匿する方式としても、本発明を同様に実施して同様の効果を得ることができる。

【0085】

さらに、上記各実施形態では、2つの認証部 12, 21 により証明書を利用した相互認証を行なう場合を説明したが、これに限らず、ICカード 10 とクライアント装置 40, 40A とに夫々共通鍵を持たせた共通鍵方式としても、本発明を同様に実施して同様の効果を得ることができる。

【0086】

また、上記各実施形態では、ICカード 10 に生体データ D が保持され、クライアント装置 40, 40A にてセンサ 24 から生体測定データ D m が入力され、両データ D, D m が照合される場合を説明したが、これに限らず、ICカード 10 にパスワード（ユーザ情報）が保持され、クライアント装置 40, 40A にて入力デバイス（キーボード又はタッチパネル等）からパスワード（ユーザ情報）が入力され、両パスワードが照合される方式としても、本発明を同様に実施して

同様の効果を得ることができる。

【0087】

また、上記各実施形態では、携帯装置を、耐タンパー性を有する IC カード 10 とした場合について説明したが、これに限らず、耐タンパー性を有して携帯可能なものであれば、携帯装置を、携帯電話や電子手帳等の任意の個人情報機器としても、本発明を同様に実施して同様の効果を得ることができる。また、携帯装置の性質に応じ、携帯装置とクライアント装置との間の通信を、無線又は赤外線（任意波長の光）等のような任意の通信方式に変形してもよい。

【0088】

その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【0089】

【発明の効果】

以上説明したように本発明によれば、携帯装置と個人認証装置との間が盗聴されても、盗聴内容から情報を読出せず、その不正使用を阻止し得る個人認証システム、それに使用される携帯装置及び記憶媒体を提供できる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態に係る個人認証システムの構成を示す模式図

【図 2】

同実施形態における動作を説明するためのフローチャート

【図 3】

同実施形態における相互認証の手順を説明するための概略図

【図 4】

本発明の第 2 の実施形態に係る個人検証システムの構成を示す模式図

【図 5】

同実施形態における動作を説明するためのフローチャート

【符号の説明】

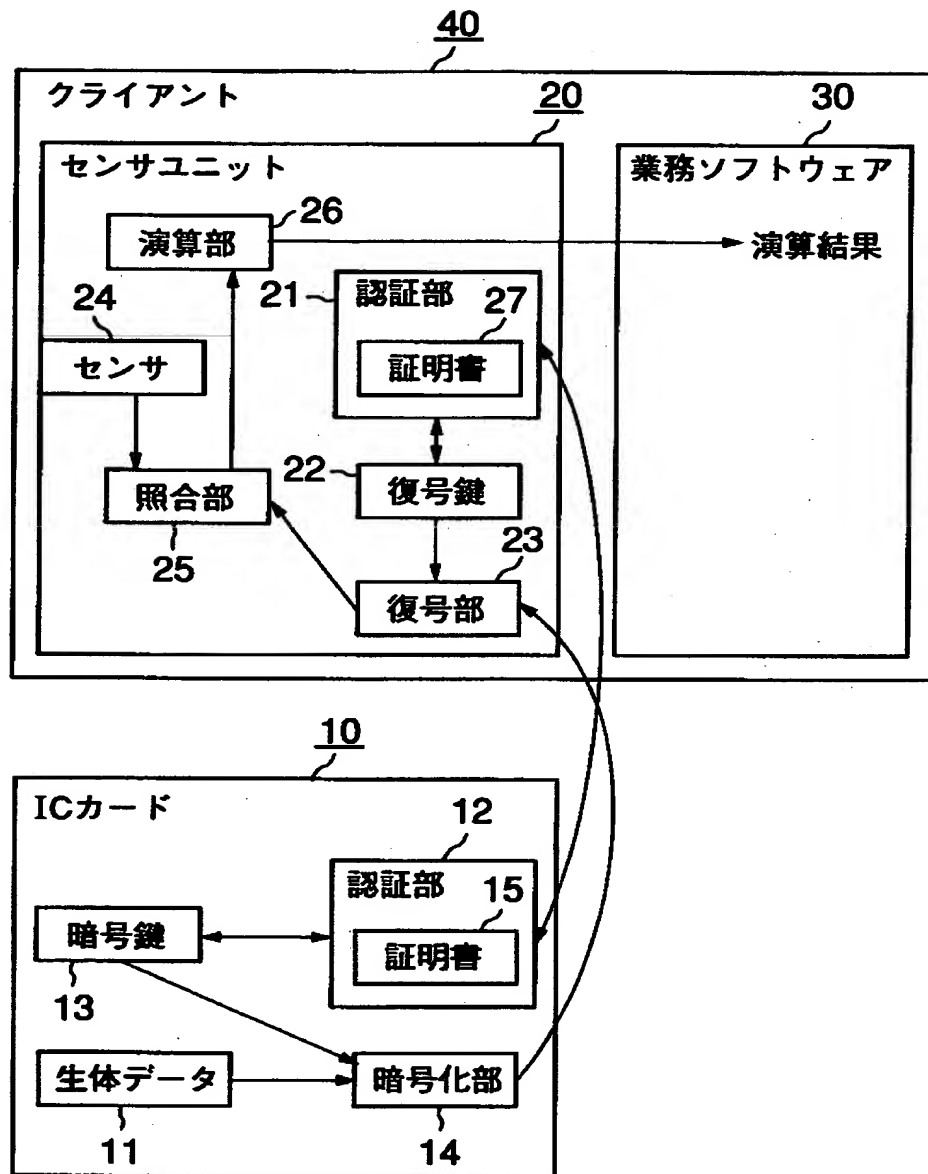
10 … IC カード

11 … 生体データ記憶部

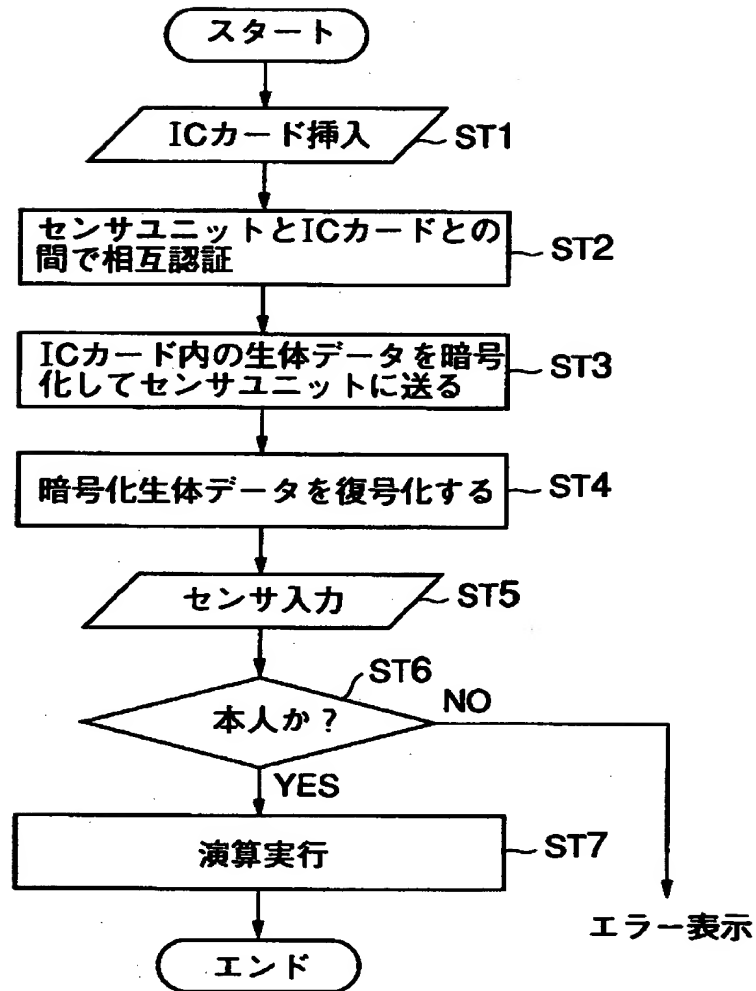
1 2, 2 1 … 認証部
1 3 … 暗号鍵記憶部
1 4, 2 9 … 暗号化部
1 5, 2 7 … 証明書
2 0, 2 0 B … センサユニット
2 0 A … クライアント認証部
2 2 … 復号鍵記憶部
2 3, 2 3 a, 2 3 b … 復号部
2 4 … センサ
2 5 … 照合部
2 6 … 演算部
2 8 a, 2 8 b … 共通鍵記憶部
3 0 … 業務ソフトウェア
4 0, 4 0 A … クライアント装置

【書類名】 図面

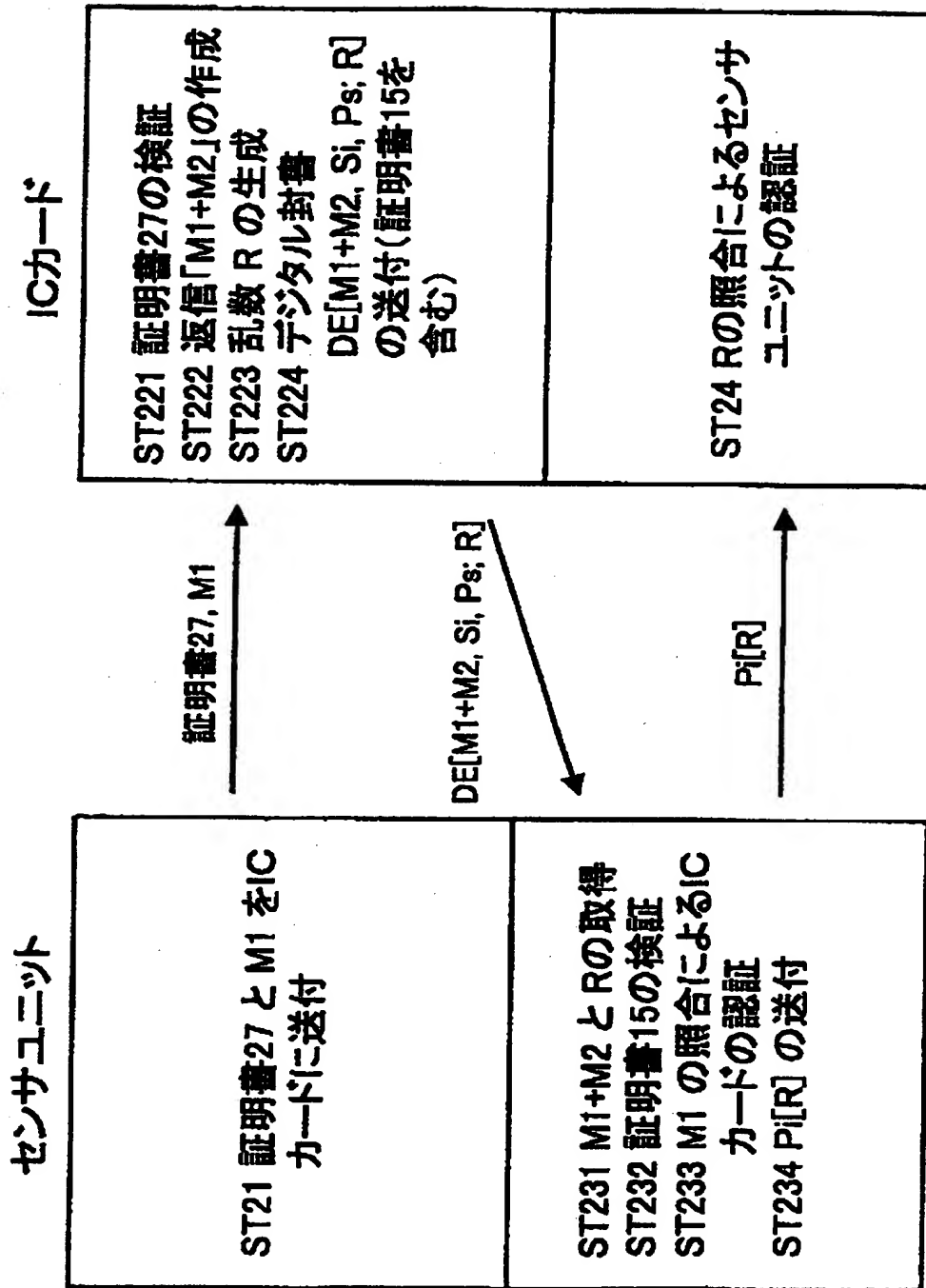
【図 1】



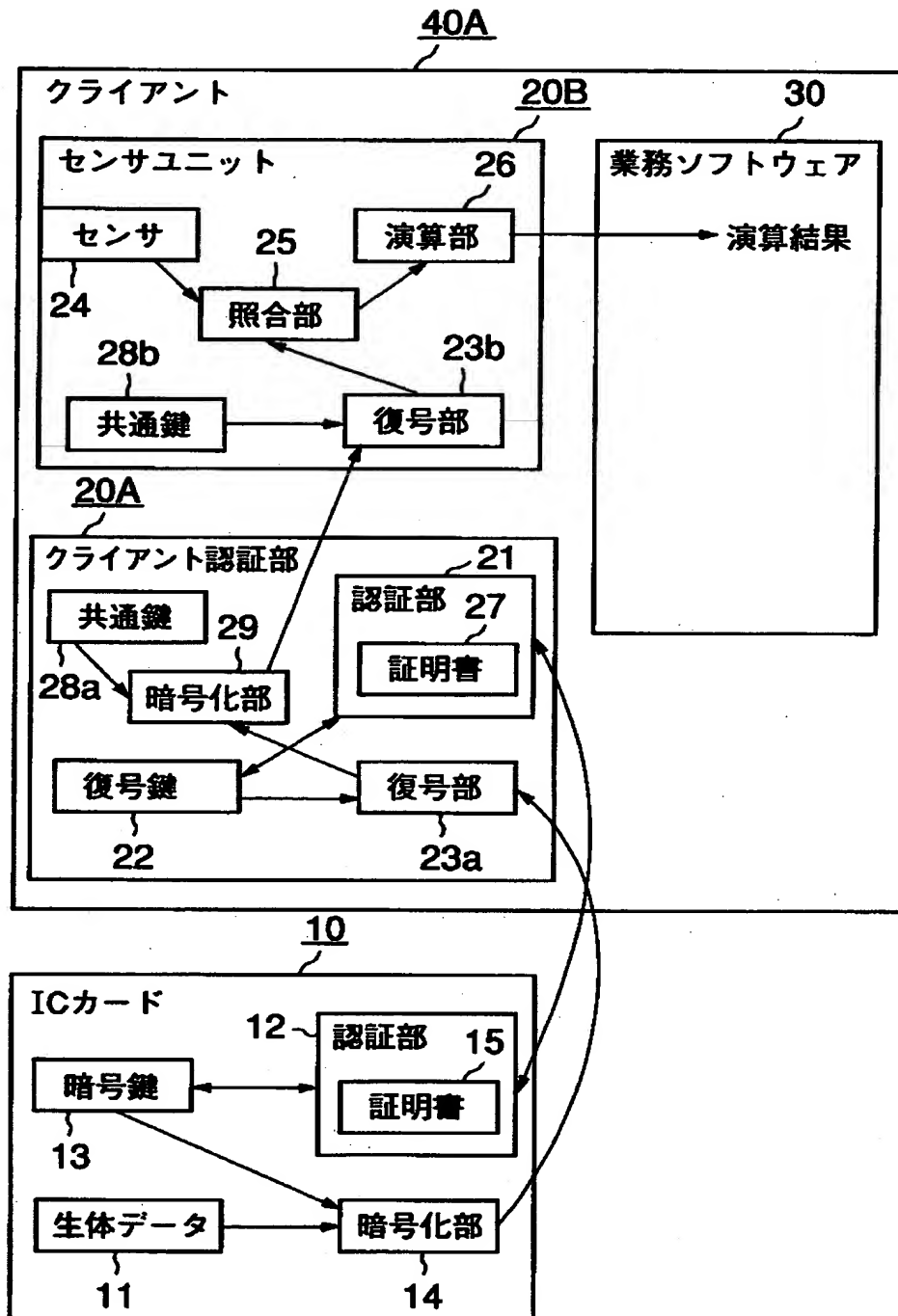
【図 2】



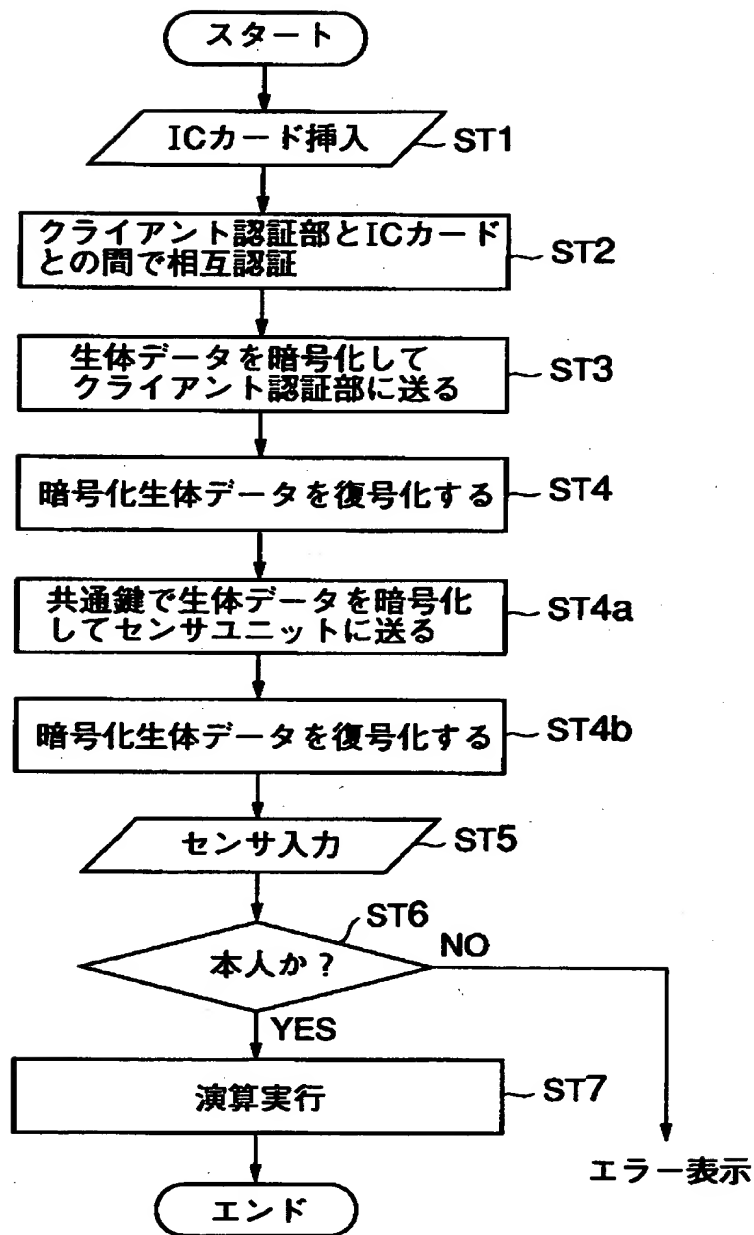
【図 3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 本発明は、携帯装置と個人認証装置との間が盗聴されても、盗聴内容から情報を読出せず、その不正使用の阻止を図る。

【解決手段】 ICカード 1 0 の暗号化部 1 4 が、個人認証が実行される時、生体データ D を暗号化し、得られた暗号文 R [D] をセンサユニット 2 0 に与え、センサユニット 2 0 の復号部 2 3 が、暗号文 R [D] を復号して生体データ D を得ると、照合部 2 5 が、この生体データ D と入力された生体測定データ D_m とを照合して本人か否かを判定する個人認証システム、それに使用される携帯装置及び記憶媒体。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000003078]

| | |
|----------|------------------|
| 1. 変更年月日 | 1990年 8月22日 |
| [変更理由] | 新規登録 |
| 住 所 | 神奈川県川崎市幸区堀川町72番地 |
| 氏 名 | 株式会社東芝 |